WHAT IS CLAIMED IS:

1. A data player for reading contents encrypted by a decoding key from a digital medium, and playing the encrypted contents by using the decoding key which is stored in a key storage unit, said data player comprising:

key obtaining means for performing mutual authentication with the key storage unit to obtain the decoding key stored in the key storage unit;

key holding means for holding the decoding key;

playback state obtaining means for monitoring the playback state of the digital medium; and

contents decoding means for decoding the encrypted contents by using the decoding key;

wherein the decoding key is obtained by the key obtaining means and stored in the key holding means, the encrypted contents read from the digital medium is decoded with the decoding key by the contents decoding means to play the contents, and the decoding key stored in the key holding means is discarded according to the playback state of the digital medium which is obtained by the playback state obtaining means.

2. The data player of Claim 1, wherein the decoding key stored in the key holding means is discarded when it is confirmed that the playback state of the digital medium has become "STOP STATE".

3. The data player of Claim 1, wherein said digital medium is a DVD.

4. The data player of Claim 2, wherein said digital medium is a DVD.

5. A data player for reading contents encrypted by a contents key and the contents key encrypted by a decoding key, from a digital medium, and playing the encrypted contents by using the decoding key which is stored in a key storage unit, said data player comprising:

key obtaining means for performing mutual authentication with the key storage unit to obtain the decoding key stored in the key storage unit;

key holding means for holding the decoding key;

playback state obtaining means for monitoring the playback state of the digital medium;

encrypted contents key decoding means for decoding the encrypted contents key by using the decoding key to obtain the contents key; and

encrypted contents decoding means for decoding the encrypted contents by using the contents key;

wherein the decoding key is obtained by the key obtaining means and stored in the key holding unit, the encrypted contents key read from the digital medium is decoded with the decoding key

by the contents key decoding means to obtain the contents key, the encrypted contents read from the digital medium is decoded by using the contents key to play the contents, and the decoding key stored in the key holding means is discarded according to the playback state of the digital media which is obtained by the playback state obtaining means.

6. The data player of Claim 5, wherein the decoding key stored in the key holding means is discarded when it is confirmed that the playback state of the digital medium has become "STOP STATE".

7. The data player of Claim 5, wherein said digital medium is a DVD.

8. The data player of Claim 6, wherein said digital medium is a DVD.

9. A key storage device comprising:

decoding key storage means for storing a decoding key for decoding encrypted data recorded on a digital medium;

key read authorization means for authorizing an external device to read the decoding key when the external device plays the encrypted data; and

key read history recording means for recording the readout record of the decoding key to the external device;

wherein, said decoding key includes available period data which is the available period for reading the decoding key; and

said key read authorization means receives a key request signal including a key read time which is the time when the external device made a request to read the decoding key, and authorizes the external device to read the decoding key after confirming that the key read time is later than the latest time amongst the read history data of the decoding key which is stored in the key read history storage means, and that the key request time is within the key read available period, and that the key read history data has been recorded by the key read history recording means.

10. The key storage device of Claim 9, wherein said key read history recording unit generates and records, in addition to the key read history data, an alteration detection code by which alteration on the key read history data can be detected.

11. The key storage device of Claim 9, wherein said key read authorization means authorizes the external device to read the decoding key after confirming that the key read history data is not altered, from the alteration detection code added to the key read history data.

12. The key storage device of Claim 10, wherein said key read

authorization means authorizes the external device to read the decoding key after confirming that the key read history data is not altered, from the alteration detection code added to the key read history data.

13. The key storage device of Claim 9, wherein:

said key read history recording means has a predetermined storage capacity; and

said key read authorization means does not authorize the external device to read the decoding key when the key read history data has reached the storage capacity of the key read history recording means.

14. A data player for reading data encrypted by a decoding key from a digital medium, and playing the data, comprising:

key obtaining means for obtaining the decoding key for decoding the encrypted data, from a key storage unit which stores the decoding key;

decoding means for decoding the encrypted data obtained from the digital medium, by using the decoding key;

data embedding means for embedding data in the data decoded by the decoding means; and

device ID code storage means for storing the device ID code of this data player;

wherein said decoding key is obtained by the key obtaining

means, and a key read time at which a request to read the decoding key was made and the device ID code of the data player are embedded in the decoded data by the data embedding means.

15. The data player of Claim 14, wherein:

said key obtaining means reads the ID code of the key storage unit which stores the decoding key, together with the decoding key, from the key storage unit; and

said data embedding means further embeds the ID code of the key storage unit in the decoded data.

16. The data player of Claim 14, wherein:

said data embedding means comprises sequence generation means for converting a pattern to be embedded to a sequence to be embedded in each video frame, and embedding means for embedding the sequence in each video frame by watermarking; and

said sequence generation means converts the pattern to be embedded to the sequence to be embedded such that short-period patterns and a long-period pattern are mixed in the sequence, said short-period patterns are obtained by dividing the pattern to be embedded according to the number of bits to be embedded in each frame and embedding the bits in each frame, and said long-period pattern is obtained by dividing the pattern to be embedded, bit by bit, and embedding the divided bits over plural frames which are plural times as many as the number into which the

pattern to be embedded is divided.

17. The data player of Claim 15, wherein:

said data embedding means comprises sequence generation means for converting a pattern to be embedded to a sequence to be embedded in each video frame, and embedding means for embedding the sequence in each video frame by watermarking; and

said sequence generation means converts the pattern to be embedded to the sequence to be embedded such that short-period patterns and a long-period pattern are mixed in the sequence, said short-period patterns are obtained by dividing the pattern to be embedded according to the number of bits to be embedded in each frame and embedding the bits in each frame, and said long-period pattern is obtained by dividing the pattern to be embedded, bit by bit, and embedding the divided bits over plural frames which are plural times as many as the number into which the pattern to be embedded is divided.

18. The data player of Claim 16, wherein said key obtaining means generates a key read history signal including the key read time and the device ID code of this data player, and transmits this signal to the key storage unit which stores the decoding key.

19. A digital contents player for reading data encrypted by a decoding key from a digital medium, and playing the data,

comprising:

key storage means for storing the decoding key for decoding the encrypted data; and

data playback means for reading the decoding key from the key storage means, and playing the data using the decoding key;

wherein said data playback means and said key storage means are removable from each other; and

when said data playback means reads the decoding key, said key storage means records key read history data including a device ID code of this digital contents player and a key read time when a request to read the decoding key was made; and

said data playback means embeds the key read time and the device ID code in the data played with the decoding key.

20. The digital contents player of Claim 19 wherein:

said data to be embedded is converted into a sequence to be embedded in each video frame, and then embedded by watermarking; and

said sequence to be embedded is a mixture of short-period patterns and a long-period pattern, said short-period patterns are obtained by dividing the pattern to be embedded according to the number of bits to be embedded in each frame and embedding the bits in each frame, and said long-period pattern is obtained by dividing the pattern to be embedded, bit by bit, and embedding the divided bits over plural frames which are plural times as

many as the number into which the pattern to be embedded is divided.

21. A key read history recording method comprising the steps of:

recording available period data which is the available period for reading a decoding key for decoding encrypted data;

recording, as a key nonuse period, a difference between a key read time when a request to read the decoding key was made and a time which has been recorded at a time that is previous and nearest to the key read time;

recording key read history data including the key read time and the device ID code of a data player; and

recording the time when use of the decoding key has ended, as an end-of-key-use time.

22. A data embedding apparatus comprising:

sequence generation means for converting a pattern to be embedded into a sequence to be embedded in each video frame; and

embedding means for embedding the sequence in each video frame by watermarking;

wherein said sequence generation means converts the pattern to be embedded into the sequence to be embedded such that short-period patterns and a long-period pattern are mixed in the sequence, said short-period patterns are obtained by dividing the pattern to be embedded according to the number of bits to be

embedded in each frame and embedding the bits in each frame, and said long-period pattern is obtained by dividing the pattern to be embedded, bit by bit, and embedding the divided bits over plural frames which are plural times as many as the number into which the pattern to be embedded is divided.

23. A data embedding apparatus comprising:

real time measuring means for outputting real time data which specifies the present time; and

data embedding means for embedding the real time data in video/audio data.

24. The data embedding apparatus of Claim 23, wherein said data embedding means embeds the real time data at the time when the video/audio data is input to this apparatus, in the video/audio data which is input in the visible/audible state to this apparatus.

25. A data embedding apparatus comprising:

real position measuring means for outputting real position data which specifies the present physical position; and

data embedding means for embedding the real position data in video/audio data.

26. The data embedding apparatus of Claim 25, wherein said data

embedding means embeds the real position data at the time when the video/audio data is input to this apparatus, in the video/audio data which is input in the visible/audible state to this apparatus.

27. A data embedding method comprising:

a real time measuring step of outputting real time data which specifies the present time; and

a data embedding step of embedding the real time data in video/audio data.

28. The data embedding method of Claim 27 wherein the real time data at the time when the video/audio data is input, is embedded in the video/audio data which is input in the visible/audible state.

29. A data embedding method comprising:

a real position measuring step of outputting real position data which specifies the present position; and

a data embedding step of embedding the real position data in video/audio data.

30. The data embedding method of Claim 29 wherein the real position data at the time when the video/audio data is input, is embedded in the video/audio data which is input in the

visible/audible state.

31. An embedded data detection apparatus for detecting embedded data from playback data in which the data is embedded by a data embedding apparatus which comprises: sequence generation means for generating a sequence in which short-period patterns and a long-period pattern are mixed, said short-period patterns being obtained by dividing a pattern to be embedded according to the number of bits to be embedded in each frame and embedding the bits in each frame, and said long-period pattern being obtained by dividing the pattern to be embedded, bit by bit, and embedding the divided values over plural frames which are plural times as many as the number into which the pattern to be embedded is divided; and data embedding means for embedding the sequence in each video frame by watermarking;

said embedded data detection apparatus comprising:

intra-frame embedded data detection means for detecting the embedded pattern from each video frame;

short-period embedded pattern detection means for calculating the embedded pattern from the embedded pattern detected by the intra-frame embedded data detection means, with reference to shirt-circuit embedded bits; and

long-period embedded pattern detection means for calculating the embedded pattern with reference to long-period embedded bits.

32. An embedded data confirming method comprising the steps of:

detecting embedded data from visible/audible data in which real time data that can specify the present time, real position data that can specify the present position, or a device ID code of a device for playing the visible/audible data is embedded; and

collating the detected data with a data base containing the history of the embedded data.

33. A playback system comprising a data output unit for outputting data, and a data player, said data player comprising decoding means for decoding input data to video/audio data which is visible or audible, real time measuring means for outputting real time data which can specify the present time, and data embedding means for embedding the real time data in the video/audio data,

wherein the real time data measured by the real time measuring means at the time when the data player plays the input data is embedded in the video/audio data.

34. The playback system of Claim 33 comprising one piece of said real time measuring means, and at least one piece of said data output unit.

35. A playback system comprising a data output unit for outputting data, and a data player, said data player comprising

decoding means for decoding input data to video/audio data which is visible or audible, real position measuring means for outputting real position data which can specify the present position, and data embedding means for embedding the real position data in the video/audio data,

wherein the real position data measured by the real position measuring means at the time when the data player plays the input data is embedded in the video/audio data.

36. The playback system of Claim 35 comprising one piece of said real position measuring means, and at least one piece of said data output unit.